(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/25937 A1

(51) International Patent Classification[7]: G06F 13/00

(21) International Application Number: PCT/US00/26843

(22) International Filing Date:
29 September 2000 (29.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/157,472 1 October 1999 (01.10.1999) US
60/206,947 25 May 2000 (25.05.2000) US

(71) Applicant *(for all designated States except US)*: **INFRAWORKS CORPORATION** [US/US]; 504 Lavaca Street, Suite 1100, Austin, TX 78701 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FRIEDMAN, George** [US/US]; 7109 Montana Norte, Austin, TX 78731 (US). **STAREK, Robert, Phillip** [US/US]; 3609 Del Robles, Austin, TX 78727 (US). **MURDOCK, Carlos** [US/US]; 4517 Avenue F, Austin, TX 78751 (US).

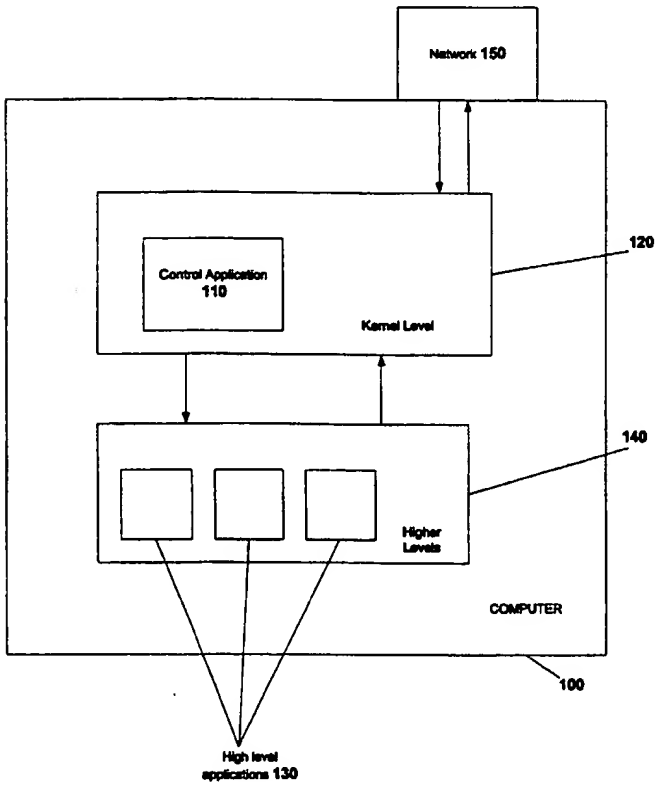
(74) Agents: **TAUFER, Paul, A.** et al.; Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103-7286 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: NETWORK/TDI BLOCKING METHOD AND SYSTEM



(57) Abstract: A network blocking method particularly applicable to a system in which protected data is segregated from other data, which allows for a network connection to be opened only by processes which do not have access to secured data in order to ensure that applications using secured data do not imperil the security of that secure data. In a preferred embodiment, network blocking method is implemented in an application (110) residing on the level (120) which monitors network requests and allows limited access to the network (150) based on whether requesting processes are secure.

WO 01/25937 A1

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *With international search report.*

NETWORK/TDI BLOCKING METHOD AND SYSTEM

Field of the Invention:

The invention relates to the protection of data stored in a computer, and more particularly, to data which has been secured and opened by non-secure applications where a high level application or operating system component acts to disable certain system resources in order to protect the security of data.

Background of the Invention:

In computer systems, processes may access many system resources, such as serial ports or connections to the Internet. In a situation in which secured data is being accessed by a non-secured application, a means must be developed by which the non-secured application can be restricted from performing operations which might compromise the security of the data.

It is known to open secure data in a system which is completely isolated from outside communications, which has no connection to means by which an unsecured application may, by accident or sabotage, compromise the secured data. It is also known to open secure data with secure applications, which are known to be free from the risk of accident or sabotage that would compromise the secured data. These solutions prevent the use of popular software applications to open secured data, or the use of a computer which is not disconnected from outside communications, and thereby are limited in their usefulness.

Summary of the Invention:

The invention discloses a network/TDI (transport driver interface) blocking method particularly applicable to a system in which secured data is transmitted to a recipient computer for use with non-secured applications. An illustrative embodiment of the invention comprises performing a security check on a process and blocking calls for use of the network if they come from a process using secured data. The tracking of secured processes may include determining whether and how often a secured process should be allowed to use a network. The security check may include determining whether the process is secured by consulting a secured process list and determining

whether the resource should be available to the process requesting use of the resource.

Further disclosed is a network blocking system, secured data transmission system using network blocking, computer-readable medium programmed to block network use, and a computer configured to block network use.

Description of the Drawings:

The invention is best understood from the following detailed description when read with the accompanying figures.

Figure 1 is an schematic diagram of a computer system operating according to an illustrative embodiment of the network blocking method of the invention.

Figure 2 is a flow chart of a network request in a computer system operating according to an illustrative embodiment of the network blocking method of the invention.

Detailed Description of the Invention:

The invention disclosed prohibits certain processes from utilizing the network resources of the computer on which they are running. These may be secured processes for example, ones which have opened secure data. In a preferred embodiment of the invention, the status of a process as secured is determined by the processes presence on a list of secured processes.

In a preferred embodiment, as shown in Fig. 1, in a computer 100, a control application 110 runs on the kernel (ring 0) level 120 and applications 130 run on higher levels 140. When applications request access to network / TDI interface 150, control application 110 monitors and handles these access requests.

As shown in Fig. 2, network blocking is accomplished by not permitting a send request to be processed for secure applications. When a send request is initiated 200, control application (110 in Fig. 1) intercepts that request, and determines the process id 210. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to access the network. The process id is used to determine whether the process is secure (not allowed to access the network) 220. If it is

secure, the request is blocked at 230. If it is not secure, then the request is passed on to the network 250.

A further illustrative embodiment of the invention is directed to a network blocking system wherein certain processes are restricted from accessing a network, according to the methods provided herein. Further disclosed is a secured data transmission system having a network blocking component to prohibit certain processes from accessing a network according to the methods provided herein. Still further disclosed is a computer-readable medium programmed to block network use according to the methods provided herein. Still further disclosed is a computer configured to include a network blocking system to block certain processes from accessing a network according to the methods provided herein.

The terms "computer", "computer system", or "system" as used herein include any electronic device having a processor or microprocessor including, without limitation, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television, such as for example, a television adapted to be connected to the Internet or an electronic device adapted for use with a television, a cellular telephone, a personal digital assistant, an electronic pager, a digital watch, or any other device capable of receiving information, such as email, from another source. A computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system.

While the invention has been described by illustrative embodiments, additional advantages and modifications will occur to those skilled in the art. Therefore the invention in its broader aspects is not limited to specific details shown and described herein. Modifications may be made without departing from the spirit and scope of the invention. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments but be interpreted within the full spirit and scope of the appended claims and their equivalents.

We claim:

1. A network blocking method for securing data comprising:

a network request detection step of detecting a network request for use of a network sent by a process;

a process identification step of determining the identity of said requesting process;

a process check step of determining if said process should be permitted to access said network; and

a permit/deny step of allowing said network request to be fulfilled if said process should be permitted to access said network and denying said network request if said process should not be permitted to access said network.

2. The method of claim 1 where said process check step comprises:

a secure process list check step of determining whether said process appears on a list of secure processes.

3. The method of claim 1, where said network requests interface is the Transport Data Interface.

4. A network blocking system wherein said network blocking system operates to determine the identity of said requesting process; determine if said process should be permitted to access said network; and allow said network request to be fulfilled if said process should be permitted to access said network and deny said network request if said process should not be permitted to access said network.

5. A secured data transmission system having network blocking system which operates to determine the identity of said requesting process; determine if said process should be permitted to access said network; and allow said network request to be fulfilled if said process should be permitted to access said network and deny said network request if said process should not be permitted to access said network.

6. A computer operably connected to a network configured to protect secure data by including a network blocking system which operates to determine the identity of said requesting process; determine if said process should be permitted to access said network; and allow said network request to be fulfilled if said process should be permitted to access said network and deny said network request if said process should not be permitted to access said network.

7. A computer-readable medium programmed to protect secure data by implementing a network blocking system which operates to determine the identity of said requesting process; determine if said process should be permitted to access said network; and allow said network request to be fulfilled if said process should be permitted to access said network and deny said network request if said process should not be permitted to access said network.

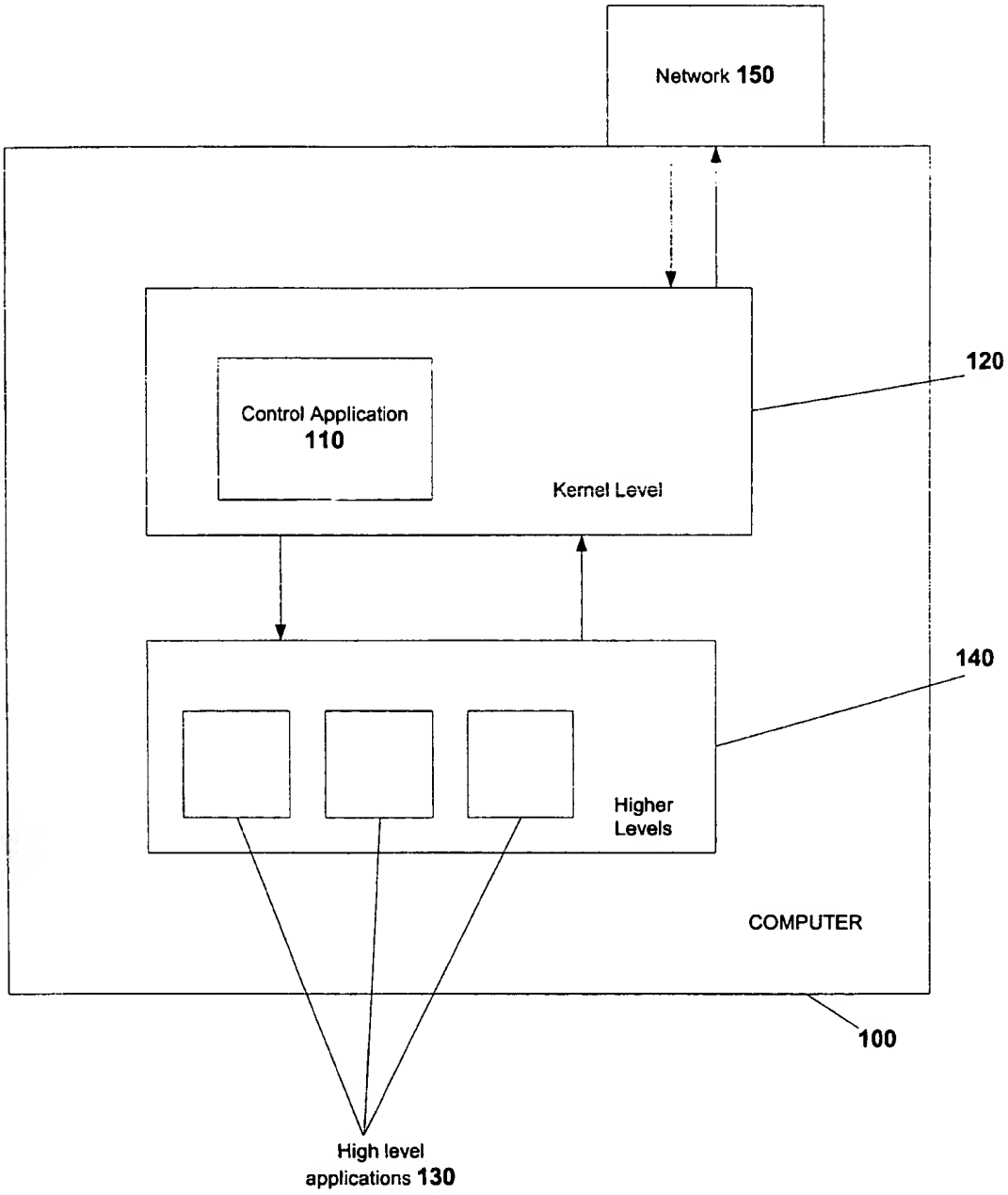

Network 150
Control Application
110
Kernel Level
120
140
Higher
Levels
COMPUTER
100
High level
applications 130

FIG. 1

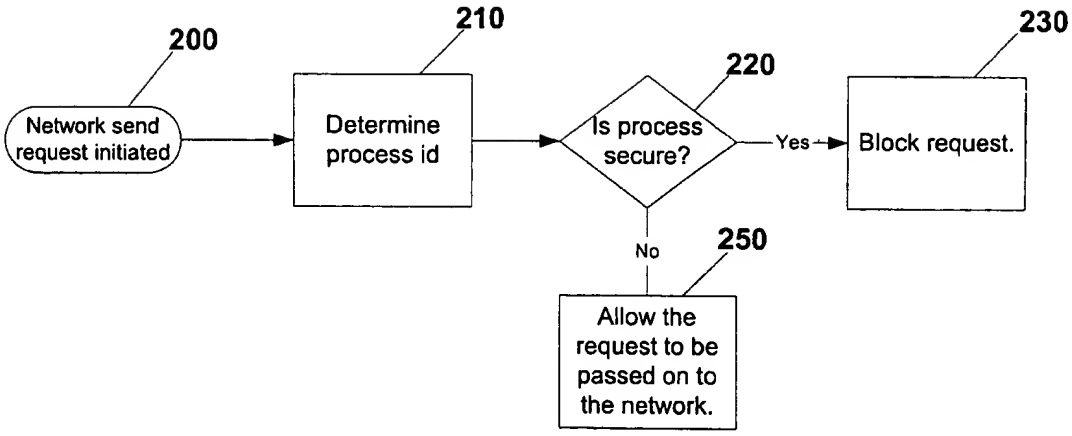

200
Network send request initiated
210
Determine process id
220
Is process secure?
Yes
230
Block request.
No
250
Allow the request to be passed on to the network.

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/26843

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00
US CL :709/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/200; 713/200, 201, 202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

None

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,067,623 A (BLAKLEY, III et al) 23 May 2000, col. 3-5	1-7
A	US 5,887,063 A (VARADHARAJAN et al) 23 March 1999, col. 1 and claim 9.	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 01 NOVEMBER 2000	Date of mailing of the international search report 28 NOV 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Hamod ARIO ETIENNE Telephone No. (703) 308-7562

Form PCT/ISA/210 (second sheet) (July 1998)*